ANALISIS YURIDIS KEJAHATAN CYBER CRIME DALAM PEMBOBOLAN MESIN ATM BANK

SKRIPSI

Oleh :

HATIALUM REHULINA BR SILALAHI
NPM. 0871010078

YAYASAN KESEJAHTERAAN PENDIDIKAN DAN PERUMAHAN
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAWA TIMUR
FAKULTAS HUKUM
PROGRAM STUDI ILMU HUKUM
SURABAYA
2012

PERSETUJUAN MENGIKUTI UJIAN SKRIPSI

ANALISIS YURIDIS KEJAHATAN CYBER CRIME DALAM PEMBOBOLAN MESIN ATM BANK

Disusun Oleh:

HATIALUM REHULINA SILALAHI
NPM. 0871010078

Telah disetujui untuk mengikuti Ujian Skripsi

Menyetujui,

Pembimbing Utama	Pembimbing Pendamping
Haryo Sulistyantoro, SH., MM	P. Handoko, SH., S.Sos., MM
NIP/NPT 19660926 199203 1 001	NIP/NPT 19620625 199103 1001

Mengetahui

DEKAN

Hariyo Sulistiyantoro,SH,MM
NIP/NPT 19620625 199103 1 001

HALAMAN PERSETUJUAN DAN PENGESAHAN SKRIPSI

ANALISIS YURIDIS KEJAHATAN CYBER CRIME DALAM PEMBOBOLAN MESIN ATM BANK

Oleh:

HATIALUM REHULINA BR SILALAHI
NPM. 0871010078

Telah dipertahankan dihadapan dan diterim oleh Tim Penguji Skripsi
Program Studi Ilmu Hukum Fakultas Hukum
Universitas Pembangunan Nasional "VETERAN" Jawa Timur
Pada Tanggal 6 Juni 2012

Menyetujui

Pembimbing Utama

Hariyo Sulistiyantoro, SH, MM
NIP/NPT 19620625 199103 1001

Pembimbing Pendamping

P. Handoko, SH., S.Sos., MM
NIP/NPT 19660926 199203 1001

Tim Penguji

1. Sutrisno,SH.,M.Hum
NIP/NPT 19601212 198803 1001

2. Subani, SH., M.Si
NIP/NPT 19510504 198303 1001

3. Hariyo Sulistiyantoro, SH, MM
NIP/NPT 19620625 1991031001

Mengetahui
DEKAN

Haryo Sulistiyantoro,SH.,MM
NIP/NPT 19620625 199103 1001

HALAMAN PERSETUJUAN DAN PENGESAHAN REVISI SKRIPSI

ANALISIS YURIDIS KEJAHATAN CYBER CRIME DALAM PEMBOBOLAN MESIN ATM BANK

Oleh:

HATIALUM REHULINA BR SILALAHI
NPM. 0871010078

Telah direvisi dan diterima oleh Tim Penguji Skripsi
Program Studi Ilmu Hukum Fakultas Hukum
Universitas Pembangunan Nasional "VETERAN" Jawa Timur
Pada tanggal 6 Juni 2012
Menyetujui

Pembimbing Utama

Hariyo Sulistiyantoro
NIP/NPT 19620625 1991031001

Pembimbing Pendamping

P. Handoko, SH., S.Sos., MM
NIP/NPT 19660926 1992031001

Tim Penguji

1. Sutrisno,SH.,M.Hum
NIP/NPT 19601212 198803 1 001

2. Subani, SH., M.Si
NIP/NPT 19510504 198303 1001

3. Hariyo Sulistiyantoro, SH, MM
NIP/NPT 19620625 1991031001

Mengetahui
DEKAN

Haryo Sulistiyantoro,SH.,MM
NIP/NPT 19620625 199103 1 001

ANALISIS YURIDIS KEJAHATAN CYBER CRIME DALAM PEMBOBOLAN MESIN ATM BANK

SKRIPSI

Diajukan Untuk Memenuhi Sebagai Persyaratan Memperoleh Gelar Sarjana Hukum Pada Fakultas Hukum UPN “VETERAN” Jawa Timur

Oleh:

HATIALUM REHULINA BR SILALAHI
NPM. 0871010078

YAYASAN KESEJAHTERAAN PENDIDIKAN DAN PERUMAHAN
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAWA TIMUR
FAKULTAS HUKUM
PROGRAM STUDI ILMU HUKUM
SURABAYA

2012

Surat Pernyataan Keaslian Penulis Skripsi

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama : Hatialum Rehulina Br Silalahi

Tempat/Tgl Lahir : Kabanjahe, 07 APRIL 1989

NPM : 0871010078

Konsentrasi : PIDANA

Alamat : JL. Bom Ginting Gg 5 Merga, Kabanjahe, SUMUT

Menyatakan dengan sebenarnya bahwa skripsi saya dengan judul: "ANALISIS YURIDIS KEJAHATAN CYBER CRIME DALAM PEMBOBOLAN MESIN ATM BANK "dalam rangka memenuhi syarat untuk memperoleh gelar Sarjana Hukum pada Fakultas Hukum Universitas Pembangunan Nasional "VETERAN" Jawa Timur adalah benar-benar hasil karya cipta saya sendiri, yang saya buat sesuai dengan ketentuan yang berlaku, bukan hasil jiplakan (plagiat).

Apabila dikemudian hari ternyata skripsi ini hasil jiplakan (plagiat) maka saya bersedia dituntut di depan Pengadilan dan dicabut gelar kesarjanaan (Sarjana Hukum) yang saya peroleh.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya dengan penuh rasa tanggung jawab atas segala akibat hukumnya.

Mengetahui
PEMBIMBING UTAMA

Surabaya, 15 Mei 2012
PENULIS

Hariyo Sulistiyantoro, SH., MM
NIP. 19620625 199103 1 001

Hatialum Rehulina Br Silalahi
NPM 0871010078

KATA PENGANTAR

Dengan mengucapkan puja dan puji syukur kehadirat Tuhan Yang Maha Esa yang telah melimpah rahmat dan karunia-Nya, sehingga penulis dapat Skripsi Penelitian ini. Di sini penulis mengambil judul "Analisis Yuridis Kejahatan Cyber Crime Dalam Pembobolan Mesin ATM Bank".

Penulisan Skripsi ini di susun guna memenuhi persyaratan untuk menempuh Gelar sarjana sesuai kurikulum yang ada di Fakultas Hukum UPN Veteran Jawa Timur. Dan dimaksudkan sebagai wahana untuk menambah wawasan serta untuk menerapkan dan membandingkan teori yang telah diterima dengan keadaan sebenarnya di lapangan. Disamping itu juga diharapkan dapat memberikan bekal tentang hal-hal yang berkaitan dengan disiplin ilmu pengetahuan.

Penyusunan Skripsi ini dapat terselesaikan atas bantuan, bimbingan dan dorongan oleh beberapa pihak. Maka pada kesempatan ini penulis mengucapkan banyak terima kasih yang terhingga kepada :

1. Bapak Hariyo Sulistiyantoro, SH , MM selaku Dekan Fakultas Hukum UPN "Veteran" Jawa Timur sekaligus sebagai Dosen Pembimbing Utama Skripsi;
2. Bapak Sutrisno, SH, M. Hum selaku Wakil Dekan I Fakultas Hukum Universitas Pembangunan Nasional "Veteran" Jawa Timur;
3. Bapak Drs. Ec. Gendut Sukarno. MS selaku Wakil Dekan II Fakultas Hukum Universitas Pembangunan Nasional "Veteran" Jawa Timur;

4. Bapak Subani, SH, MSi selaku Ketua Program Studi Ilmu Hukum Fakultas Hukum UPN “Veteran” Jawa Timur;
5. Bapak Panggung Handoko, SH., S.Sos., MM Selaku Pembimbing dua
6. Seluruh Bapak dan Ibu Dosen, serta Staff Fakultas Hukum UPN “Veteran” Jawa Timur yang telah membimbing dalam penulisan serta penyusunan Skripsi ini sampai dengan selesai.
7. Bapak Kompol Bambang Suryanto, SH Selaku Ketua Unit IV Cyber Crime Subdit II Fismondev Ditreskrimsus, Bapak Bripka Wisnu Polda Jatim, yang telah membimbing dan mengarahkan sehingga penulis dapat menyusun Skripsi ini hingga selesai.
8. Bapak (Alm) dan Mama saya, serta kepada ke 3 saudara kandung saya Lisbet Silalahi, Hana Silalahi, Samuel Sabar Pandapotan Rumah Singap Silalahi tidak ketinggalan juga kepada kakak sepupu saya Monika Simbolon, Kak Lena, Abg Andry, Wendy Simbolon yang telah memberikan doa dan dukungannya sehingga penulis dapat menyelesaikan Skripsi ini;
9. Senior Aktifis se Indonesia Khusus nya kepada Abang Atma, Abg Andra (Trisakti/Ketua Gemanusa), Mr Obama (HMI), Abg Nando, Abg Sufriansyah Pasaribu (Deklaratoir BEMNUS), Abg Albert, Kak Marchel MM, Abg M. Yusuf Sahide(KPK Watch Indonesia), Abg MA. Yakin Simatupang (Ketua PB PMII), Mas Andik, Abg Almunazir, dari Sabang Sampai Merauke yang telah memberikan dukungan dan arahannya kepada saya.
10. Teman-teman mahasiswa khusus nya kepada Mbak Diswo, Andyna, Fitra, dhito, dan lain-lain yang tidak dapat penulis sebutkan satu persatu yang telah

membantu dan memberikan saran sebagai masukan di dalam penulisan Skripsi ini hingga selesai.

Penulis menyadari bahwa penulisan Skripsi ini masih jauh dari sempurna, oleh karena itu saran dan kritik yang sifatnya membangun penulis harapkan guna memperbaiki dan menyempurnakan penulisan yang selanjutnya, sehingga Skripsi Penelitian ini dapat bermanfaat bagi masyarakat dan bagi yang memerlukan nya.

Surabaya, Mei 2012

Penulis

DAFTAR ISI

HALAMAN JUDUL i

HALAMAN PERSETUJUAN PROPOSAL SKRIPSI..... ii

HALAMAN PERSETUJUAN DAN PENGESAHAN REVISI SKRIPSI iii

HALAMAN PERSETUJUAN DAN PENGESAHAN SKRIPSI..... iv

SURAT PERNYATAAN KEASLIAN PENULIS SKRIPSI v

KATA PENGANTAR..... iv

DAFTAR ISI vii

DAFTAR LAMPIRAN viii

ABSTRAK..... ix

BAB I PENDAHULUAN..... 1

1.1. Latar Belakang..... 1

1.2. Rumusan Masalah..... 6

1.3. Tujuan Penelitian 6

1.4. Manfaat Penelitian 7

1.5. Kajian Pustaka 8

1.5.1. Pengertian 8

a. Cyber Crime 8
b. Cyber Space 8
c. Cyber Law 9
d. Bank 9
e. Hukum 10
f. Kartu ATM 10
g. Pemegang Kartu Kredit (Kartu Kredit) 11
h. Penyalahgunaan Komputer (Internet) 11
i. Pihak Ketiga 11
j. Internet 12
1.5.2. Transaksi Elektronik 12
1.5.3. Tindak Pidana Teknologi Informasi (Cyber Crim) Dalam Undang - Undang Nomor 11 Tahun 2008 Tentang ITE 13
1.5.4. Sejarah Komputer 19
1.5.5. Internet Melahirkan Kejahatan Komputer 21
1.5.6. Kejahatan Perbankan Dalam Problematika Perkembangan Hukum Ekonomi Dan Teknologi 23
1.5.7. Pembedaan Hacker Dan Cracker 24
1.5.8. Jenis-Jenis Cyber Crime Berdasarkan Modus Operandinya 32
1.5.9. Jenis-Jenis Cyber Crime Berdasarkan Motifnya 35
1.5.10. Jenis-Jenis Cyber Crime Berdasarkan Korbannya 36
1.3.11. Kejahatan 37
1.5.12. Hubungan KUHP Dengan Cyber Crime 38

1.5.13. Tindak Pidana Perbankan 40

1.6. Metodologi Penelitian 40

a. Jenis Dan Tipe Penelitian 40

b. Sumber Data 41

c. Metode Pengumpulan Data..... 42

d. Metode Pengolahan Data..... 43

e. Metode Analisis Data 43

f. Sistematika Penulisan..... 44

BAB II Akibat Hukum Dari Pembobolan Mesin ATM Bank Dalam Hukum Pidana..... 45

2.1. Pengertian Hukum..... 45

2.2. Akibat Hukum Dari Pembobolan Mesin ATM Bank Dalam Hukum Pidana..... 54

BAB III Perlindungan Hukum Bagi Nasabah Yang Menjadi Korban Pembobolan Mesin ATM Bank 58

3.1. Perlindungan Hukum Yang diberikan Pihak Bank kepada Pengguna ATM yang menjadi Nasabahnya..... 58

3.2. Perlindungan Hukum Bagi Nasabah Yang Menjadi Korban Pembobolan Mesin ATM Bank 65

BAB IV KESIMPULAN DAN SARAN..... 71

4.1. Kesimpulan..... 71

4.2. Saran..... 72

DAFTAR PUSTAKA

LAMPIRAN

UNIVERSITAS PEMBANGUNAN NASIONAL"VETERAN" JAWA TIMUR
FAKULTAS HUKUM

Nama Mahasiswa : Hatialum Rehulina Silalahi

NIP : 0871010078

Tempat Tanggal Lahir : Kabanjahe, 07 April 1989

Program Studi : Strata 1 (S1)

Judul Skripsi :

ANALISIS YURIDIS KEJAHATAN CYBER CRIME DALAM PEMBOBOLAN MESIN ATM BANK

ABSTRAKSI

Penelitian ini bertujuan untuk mengetahui bagaimana akibat hukum terhadap pembobolan mesin ATM bank dalam Hukum Pidana serta bagaimana perlindungan hukum terhadap nasabah korban pembobolan ATM Bank. Penelitian ini menggunakan metode normatif empiris (holistik) melalui wawancara. Sumber data diperoleh dari literatur-literatur, karya tulisan ilmiah dan perundang-undangan yang berlaku. Analisa data menggunakan analisa kualitatif.

Hasil penelitian dapat disimpulkan bahwa pembobolan ATM bank yang dilakukan oleh pelaku dapat di hukum dalam hukum pidana atau dalam KUHP serta dapat dijerat dengan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronika. Sedangkan bagi nasabah / korban pembobolan ATM bank pihak bank selaku pelaku pemberi jasa dapat mengganti kerugian dari nasabah korban pembobolan ATM bank.

Kata Kunci, Cyber Crime, Pembobolan ATM Bank.

BAB I

PENDAHULUAN

1.1. Latar Belakang

Di zaman era globalisasi ini, banyak teknologi informasi maupun teknologi telekomunikasi yang semakin terkemuka hampir banyak teknologi maupun alat dan elektronik yang tiap saat bermunculan dan berganti model (type). kita ketahui berbagai macam barang-barang teknologi seperti HP, Laptop, Internet dan lain sebagainnya. Apalagi dalam kehidupan yang serba canggih sekarang ini, kita telah mengenal ATM. Karena dalam penggunaanya sangat lah efesien dan efektif.

Dengan adannya teknologi semacam ini kebutuhan kita dapat lebih mempermudah cara kerja kita bukan hanya itu saja dalam hal pengambilan uang melalui ATM juga lebih mempermudah dan tidak banyak memakan waktu untuk mengambil uang secara cepat dan nyaman. Namun semakin tingginnya perputaran uang lewat ATM tanpa kita sadari dalam kehidupan sehari-hari muncul berbagai kejahatan.

Salah satu titik kelemahan ATM yang menjadi targetan kejahatan adalah dengan modus pencurian PIN atau memanipulasi kartu ATM si nasabah.[1] Kita tidak mengetahui bagaimana proses ini berlangsung,

[1] Ronnny Prasetyo, Pembobolan ATM , Tinjauan Hukum Perlindungan Nasabah Korban Kejahatan Perbankan , Prestasi Pustaka, Cet I, Jakarta, 2004, hlm. 1-2

beberapa kasus pembobolan bank di Indonesia melalui ATM, yaitu Bank CIMB Niaga. Kasus pembobolan ini telah menjadi buah bibir dan pembicaraan hangat di media massa. Dan ini adalah salah satu bentuk kejahatan teknologi, yang dapat disebut cyber crime. Terkadang hal semacam ini sangat sulit untuk diungkapkan karena dilakukan oleh penjahat bank yang memiliki pengetahuan teknologi yang cukup tinggi, dengan pengetahuan teknologi yang dimiliki oleh pelaku tersebut maka kemungkinan besar pelaku kejahatan Cyber Crime dapat melihat nomor PIN kita.

Kejahatan seperti ini dapat dikategorikan sebagai tindakan pencurian / penipuan yang terdapat dalam KUHP dan UU No. 11 tahun 2008 tentang Informasi Transaksi Elektronik yang untuk selanjutnya di sebut UU ITE. Siapapun penduduk baik di kota maupun sekalipun di desa yang telah memiliki ATM (Anjungan Tunai Mandiri) apalagi di kota besar, di dalam dompetnya pasti terdapat setidaknya sebuah kartu plastik berpita magnet tersebut sering yang disebut dengan ATM. Alangkah terkejutnya kita, semua ketika belakangan ini berturut-turut terjadi kasus pembobolan ATM yang menimpa banyak nasabah bank yang terkemuka, sehingga menimbulkan banyak kerugian dapat mencapai nilai miliaran rupiah. Pihak kepolisian mensinyalir, pembobolan dana nasabah lewat

Berkaitan dengan hal tersebut, selanjutnya peneliti mencoba telusuri dan kaji mengenai cybercrime, khususnya kasus pembobolan mesin ATM bank dalam tinjauan hukum cybercrime.

Contoh kasus yang ada Jakarta dan di bali kembali dilaporkan bahwa seorang nasabah kehilangan uang dalam rekening ATM mereka, akibat penarikan lewat mesin yang di ATM Bali. Polisi tengah menyelidiki kemungkinan keterlibatan orang dalam dari bank-bank yang menjadi sasaran pembobolan ATM. Menurut laporan Polda Bali, aksi pembobolan ATM terjadi pada BCA, Bank Mandiri, BNI, BRI, dan Bank Permata. Sementara menurut data Bank Indonesia (BI), Rekening yang dibobol lewat 13 ATM terutama berlokasi di Bali dalam waktu hampir bersamaan bahkan mencapai 236 rekening. Terkait dengan munculnya sejumlah laporan yang menghubungkan kejahatan ini dengan keterlibatan sindikat asing, kepolisian menyatakan masih terus menyelidiki.

Kejahatan di dunia maya (cyber) dewasa ini tingkat kerawanannya dan kerugiannya sudah melebihi dunia nyata, bila seseorang perampok bank paling tinggi merampas uang senilai puluhan atau ratusan juta rupiah maka pencoleng online bisa menjarah jutaan bahkan miliaran dollar dalam waktu singkat secara cepat. Kepala interpol memprediksikan bahwa kejahatan dunia maya (cyber) akan muncul sebagai ancaman kriminal terbesar bagi Asia, dan masalah-masalah yang ada sekarang menunjukkan kecenderungan terus memburuk dan semakin liar. Pada

dunia kejahatan modern, pencurian bukan lagi hanya berupa pengambilan barang / material yang berwujud saja, tetapi juga termasuk pengambilan data secara tidak sah.[2]

Kejahatan dalam dunia maya (cyberspace) menghadirkan berbagai persoalan baru dan berat dengan skala internasional dan sangat kompleks dalam upaya pemberdayaan hukum agar bisa menanganinya. Kejahatan – kejahatan ekonomi termasuk kartu ATM dan pencurian uang merupakan masalah kedua yang sangat mengkhawatirkan bagi dunia perbankan, khususnya yang dilakukan Asia. Dengan berbagai harapan berupa penyelundupan manusia, obat bius, terorisme, pencurian uang lewat kartu ATM maupun internet, penemuan kasus suap dan korupsi hampir setiap hari terungakp menghiasi media – media massa di Asia, bangsa – bangsa Asia perlu sering bekerja sama dengan penuh komitmen untuk menghadapi segala bentuk kejahatan lama maupun baru di bidang ekonomi perbankan yang semakin kronis ini.

Selain dari pada contoh kasus pembobolan mesin ATM yang ada di Jakarta dan Bali tak ketinggalan juga ada beberapa kasus pembobolan mesin ATM yang dilakukan oleh Pihak ke tiga salah satu nya adalah pembobolan mesin ATM Bank BNI Cabang Pemuda Surabaya. Dalam hal

[2] Ibid, hlm. 13

ini pelaku menggunakan alat semprot ke bagian CCTV dan pelaku tersebut memakai topi untuk menutupi dirinya. Nasabah yang melaporkan kejadian ini bernama Ni Wayan Sami Ernawati kerugian sebesar 151 Juta. Modus Operandinya dilakukan dengan cara memindahkan uang nasabah ke nomor rekening orang yang berbeda-beda tempat atau yang berada di luar kota.

> Menurut Bapak Bripka Wisnu Murti dugaan sementara bahwa uang yang dipindah kan ke rekening orang-orang tersebut adalah orang yang garis keras tetapi belum jelas apakah orang garis keras tersebut atau salah satu pihak Bank tersebut atau para hacker yang melakukan aksi tersebut dengan memakai internet di luar agar dapat menghilangkan jejak sedangkan untuk pemindahan uang tersebut ke rekening orang yang berbeda-berbeda dilakukan dengan cara mencuri atau mengcopy Nomor PIN nasabah tersebut dengan sebuah alat yang disebut dengan Skimmer sampai saat ini pihak aparat masih dalam proses penyidikan dan akan di upayakan bagaimana pihak bank supaya mengganti kerugian nasabah tersebut.[3]

Jadi pembobolan bank yang dilakukan oleh pihak ketiga seringkali mengandung unsur kejahatan. Belajar dari kenyataan – kenyataan yang terjadi dimasyarakat, maka saya terdorong untuk melakukan penelitian terhadap "Analisis Yuridis Kejahatan Cyber Crime Dalam Pembobolan Mesin ATM Bank." Dari studi awal yang saya lakukan banyak dilakukan oleh pihak – pihak yang telah menguasai komputer (internet).

Menegakkan sistem hukum dan perundang – undangan merupakan tugas dan kewajiban yang memang sangat berat, yang harus dilaksanakan oleh para praktisi hukum. Berbagai upaya dilakukan baik melalui

[3] Wawancara dengan Bapak Bripka Wisnu Murti, Pada Tanggal 6 Januari 2012, Di Polda Jatim Surabaya

pemberdayaan dari pihak masyarakat maupun usaha – usaha merevisi peraturan perundang – undangan dalam pembenahan sistem hukum itu sendiri.

1.2. Rumusan Masalah

Berdasar uraian dalam latar belakang, maka dapat dirumuskan permasalahan dalam penelitian ini sebagai berikut :

a. Apa Akibat Hukum dari Pembobolan Mesin ATM Bank menurut Hukum Pidana?

b. Bagaimana Perlindungan Hukum bagi Nasabah yang menjadi Korban Pembobolan ATM bank ?

1.3. Tujuan Penelitian

a. Tujuan dari penulisan skripsi ini adalah untuk mengetahui apa akibata hukum dari pembobolan ATM bank dalam hukum pidana.

b. Untuk mengetahui bagaimana perlindungan hukum terhadap nasabah korban pembobolan ATM bank.

1.4. Manfaat Penelitian

a. Manfaat Teoritis

Hasil penelitian ini diharapkan dapat mengembangkan ilmu pengetahuan khususnya dibidang hukum ilmu teknologi serta dapat membedakan tindak pidana umum dan tindak pidana khusus, terkait mengenai kejahatan cyber crime tentang pembobolan mesin ATM bank

b. Manfaat Praktis

(1) Untuk Menambah pengetahuan mengenai tindak pidana kejahatan Informasi Transaksi Elektronik khususnya kejahatan cyber crime tentang pembobolan mesin ATM bank.

(2) Bagi Aparat Penegak Hukum khususnya bagi Kepolisian, Jaksa, Hakim agar selalu dapat meningkatkan perlindungan hukum bagi seluruh masyarakat yang dirugikan khususnya bagi nasabah korban pembobolan mesin ATM bank di Indonesia serta dapat memprioritaskan kepentingan hukum bagi nasabah korban pembobolan mesin ATM bank yang berada di Indonesia.

1.5. Kajian Pustaka

1.5.1. Pengertian

a. Cybercrime

Cybercrime adalah tindak criminal yang dilakukan dengan menggunakan teknologi computer sebagai alat kejahatan utama. Cybercrime merupakan kejahatan yang memanfaatkan perkembangan teknologi computer khusunya internet. Cybercrime didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi computer yang berbasis pada kecanggihan perkembangan teknologi internet.[4] Cyber Crime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia internasional. Volodymyr Golubev menyebutnya sebagai the new form anti-social behavior.

Beberapa julukan/sebutan lainnya yang cukup keren diberikan kepada jenis kejahatan baru ini dalam berbagai tulisan, antara lain, sebagai kejahatan dunia maya (cyber space/virtual space offence), dimensi baru dari high tech crime, dimensi baru dari transnational crime,dan dimensi baru dari white collar crime.Cyber crime (selanjutnya disingkat CC) merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini.[5]

b. Cyber Space

Kegiatan melalui media sistem elektronik, yang disebut juga ruang siber (cyber space), meskipun bersifat virtual dapat dikategorikan sebagai tindakan atau perbuatan hukum yang nyata.Secara yuridis kegiatan pada ruang siber tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional saja sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum.Kegiatan dalam

[4] Wordpress, Roniarmardi, Defenisi Cyber Crime. Com diakses pada tanggal 6 Januari 2012 pukul 21.00 WIB

[5] Barda Nawawi Arief, Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime Di Indonesia, PT Raja Grafindo Persada, Jakarta, 2006, hlm 1

ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik.[6]

c. Cyber Law

adalah aspek hukum yang istilahnya berasal dari Cyberspace Law, yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet/elektronik yang dimulai pada saat mulai "online" dan memasuki dunia cyber atau maya. Pada negara yang telah maju dalam penggunaan internet/elektronik sebagai alat untuk memfasilitasi setiap aspek kehidupan mereka, perkembangan hukum dunia maya sudah sangat maju. Sebagai kiblat dari perkembangan aspek hukum ini, Amerika Serikat merupakan negara yang telah memiliki banyak perangkat hukum yang mengatur dan menentukan perkembangan Cyber Law.[7]

Menurut Undang-undang Nomor 10 Tahun 1998 pasal 1 mengatakan Perbankan adalah segala sesuatu yang menyangkut tentang bank,mencakup kelembagaan, kegiatan usaha, serta cara dan proses dalam melaksanakan kegiatan usahanya.[8]

d. Bank

Bank adalah salah satu lembaga keuangan yang terpenting bagi masyarakat dalam suatu negara. Dalam sistem perekonomian ini, terdapat Bank Umum dan Bank Perkreditan Rakyat, dimana Bank tersebut dijalankan dan di miliki oleh negara ataupun oleh swasta. Disamping itu

---

[6] Departemen Komunikasi Dan Informatika Republik Indonesia, Buku Panduan Untuk Memahami UU No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, 2008, Hal 94-95

[7] http://jendralberita.wordpress.com.Diakses pada tanggal 08 april 2012 pukul 00:22 WIB

[8] Ronnny Prasetyo, op cit. hlm. 197,

terdapat Bank Sentral yang mengatur serta mengawasi sistem kerja semua Bank tersebut dan membantu mencapai tujuan ekonomi dalam pembangunan perekonomian nasional, yakni agar ekonomi masyarakat semakin adil dan merata. Adapun pengertian Bank itu sendiri menurut Undang – Undang Nomor 10 Tahun 19998 Tentang Perbanka adalah :

"Badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkan kepada masyarakat dalam bentuk kredit dan atau bentuk laiinya dalam angka meningkatkan taraf hidup rakyat banyak.[9]

e. Hukum

Hukum berfungsi sebagai perlindungan kepentingan manusia.Agar kepentingan manusia terlindungi, hukum harus dilaksanakan.[10] Jadi, perlindungan hukum merupakan perlindungan yang diberikan oleh hukum maupun undang-undang untuk melindungi kepentingan manusia agar kehidupan manusia dapat berlangsung normal, tenteram, dan damai.

f. Kartu ATM (Kartu Kredit)

Kartu ATM adalah kartu plastik yang diberikan oleh bank yang dapat digunakan oleh pemegangnnya untuk membeli barang-barang dan jasa secara tunai maupun kredit dan bisa berguna sebagai penarikan uang secara tunai.Sedangkan ATM (Automatic Teller Machine) adalah

[9] Ibid, hlm. 11
[10] Ibid.

mesin/komputer yang digunakan oleh bank untuk melayani transaksi keuangan seperti penyetoran uang , pengambilan uang tunai,pengecekan saldo, transfer uang dari satu rekening ke rekening lainnya, serta transaksi keuangan sejenis lainnya secara elektronik.[11]

g. Pemegang kartu ATM (Kartu Kredit)

Pemegang Kartu ATM adalah pemilik utama (nasabah) kartu ATM yang dapat melakukan transaksi keuangan melalui ATM, baik untuk penarikan uang secara tunai maupun pembelian/pembayaran barang–barang dan jasa secara tunai maupun kredit.[12]

h. Penyalahgunaan komputer (Internet)

Didefenisikan secara luas sebagai suatu kejadian yang berhubungan dengan teknologi komputer yang seorang korban menderita atau akan telah menderita kerugian dan seorang pelaku dengan sengaja memperoleh keuntungan atau akan telah memperoleh keuntungan.[13]

i. Pihak ketiga

Yang dimaksud disini yaitu hacker dan phreaker yaitu orang yang pekerjaannya memasuki atau mengakses secara tidak sah suatu sistem

[11] Ibid.
[12] Ibid, hlm. 12
[13] Ibid.

komputer maupun internet. Ada dua cara hacker mendapatkan data-data tentang kartu ATM (Kartu Kredit), yaitu:

1. Melalui komputer bank dan perusahaan kartu kredit
2. Transhing, yaitu suatu cara dimana hacker membongkar/memeriksa sampah perusahaan-perusahaan atau tokoh-tokoh yang diperkirakan menerima melalui ATM (Kartu Kredit).[14]

j. Internet

Internet adalah jaringan luas dari komputer ,yang lazim disebut dengan worldwide network.[15] Internet juga merupakan sumber informasi dan alat komunikasi serta hiburan. Dengan Internet kita juga dapat melakukan transaksi perbankkan (Internet Banking): membuka kartu ATM maupun transfer rekening antar bank.

1.5.2. Transaksi Elektronik

UU ITE Bab 1 Ketentuan Umum Pasal 1 angka 2 menyebutkan Transaksi Elektronik adalah perbuatan hukum yang dilakukan menggunakan Komputer, jaringan Komputer , dan/atau media elektronik lainnya. Penjelasan transaksi secara elektronik, pada dasarnya adalah perikatan ataupun hubungan hukum yang dilakukan secara elektronik dengan memadukan jaringan dari sistem elektronik berbasiskan komputer

[14] Ibid.
[15] Ibid.

dengan sistem komunikasi, yang selanjutnya difasilitasi oleh keberadaan jaringan komputer global atau internet.

1.5.3. Tindak Pidana Teknologi Informasi (Cyber Crime) Dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik

Pengaturan hukum terhadap Tindak Pidana di Bidang Teknologi Informasi diatur didalam UU Nomor 11 Tahun 2008 tentang Informasi dan Teknologi Elektronik. Di dalam UU Nomor 11 Tahun 2008 tentang Informasi dan Teknologi Elektronik (ITE) (selanjutnya ditulis: UU No.11 Tahun 2008) dimuat ketentuan tentang unsur-unsur tindak pidana (Perbuatan yang Dilarang) di bidang ITE,antara lain dalam ketentuan Pasal 27 sampai dengan Pasal 36 UU No.11 Tahun 2008 berbunyi sebagai berikut :

> "(1) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
>
> (2) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan /atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.
>
> (3) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
>
> (4) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman."

Ketentuan Pasal 28 ayat (1) dan ayat (2) UU No.11 Tahun 2008 berbunyi sebagai berikut :

"(1) Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dan Transaksi Elektronik.

(2) Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan / atau kelompok masyarakat tertentu berdasarkan atas suku, agama, dan antargolongan (SARA)".

Ketentuan Pasal 29 UU No. 11 Tahun 2008 berbunyi sebagai berikut :

"Setiap orang dengan segaja dan tanpa hak mengirimkan informasi Elektronik dan/ atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi."

Ketentuan Pasal 30 ayat (1), ayat (2), dan ayat (3) UU No.11 Tahun 2008 berbunyi sebagai berikut :

"(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun.

(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

(3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar , menerobos, melampaui, atau menjebol sistem pengamanan."

Ketentuan Pasal 31 ayat (1) dan ayat (2) UU No. 11 Tahun 2008 berbunyi sebagai berikut :

"(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik orang lain.

(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu komputer dan/atau Sistem Elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan."

Ketentuan Pasal 32 ayat (1) dan ayat (2) UU No. 11 Tahun 2008 berbunyi sebagai berikut.

"(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik.

(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak."

Ketentuan Pasal 33 UU No. 11 Tahun 2008 berbunyi sebagai berikut :

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya."

Ketentuan Pasal 34 ayat (1) UU No. 11 Tahun 2008 berbunyi sebagai berikut :

"(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:

a. Perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
b. Sandi lewat Komputer; Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik mejadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33."

Ketentuan Pasal 35 UU No. 11 Tahun 2008 berbunyi sebagai berikut :

> "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang autentik."

Ketentuan Pasal 36 UUNo. 11 Tahun 2008 berbunyi sebagai berikut :

> "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi orang lain."

Berkenaan dengan unsur-unsur tindak pidana di bidang ITE tersebut, di dalam UU No. 11 Tahun 2008 dirumuskan juga sejumlah ketentuan pidana di bidang ITE tercantum didalam Pasal 45 sampai dengan Pasal 52 adapun ketentuannya adalah sebagai berikut;

Ketentuan Pasal 45 ayat (1), (2), dan (3) UU No. 11 Tahun 2008 berbunyi sebagai berikut :

> "(1) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
>
> (2) Setiap orang yang memenuhi unsur sebagaimana dimaksud Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
>
> (3) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah)."

Ketentuan Pasal 46 ayat (1), (2), dan (3) UU No. 11 Tahun 2008 berbunyi sebagai berikut :

"(1) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta).

(2) Setiap orang yang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7(tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta).

(3) Setiap orang ,emenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) di pidana dengan pidana penjara paling lama 8(delapan) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta)."

Ketentuan Pasal 47 UU No.11 Tahun 2008 berbunyi sebagai berikut :

"Setiap orang yang memenuhi unsur sebagaimana yang dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah)

Ketentuan Pasal 48 ayat (1), (2), dan (3) UU No.11 Tahun 2008 berbunyi sebagai berikut :

"(1) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.0000,00 (dua miliar rupiah)

(2) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp 3.000.000.000,00 (tiga miliar rupiah).

(3) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 5.000.000.000,00 (lima miliar rupiah)."

Ketentuan Pasal 49 UU No.11 Tahun 2008 berbunyi sebagai berikut :

"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33,dipidana dengan pidana penjara paling lama 10(sepuluh) tahun dan/atau denda paling banyak Rp 10.000.000.000,00 (sepuluh miliar rupiah)."

Ketentuan Pasal 50 UU No.11 Tahun 2008 berbunyi sebagai berikut.

"Setiap orang yang memenuhi unsur sebagaimana yang dimaksud dalam Pasal 34 ayat (1) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 10.000.000.000,00 (sepuluh miliar rupiah)."

Ketentuan Pasal 51 ayat (1) dan (2) UU No.11 Tahun 2008 berbunyi sebagai berikut :

"(1) Setiap orang yang memenuhi unsur sebagaimana yang dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (du belas) tahun dan/atau denda paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah)

(2) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah)."

Ketentuan Pasal 52 ayat (1), (2), (3), dan (4) UU No.11 Tahun 2008 berbunyi sebagai berikut :

"(1) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak dikenakan pemberatan sepertiga dari pidana pokok.

(2) Dalam hal perbuatan sebagimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang dugunakan untuk layanan publik dipidana dengan piadana pokok ditambah sepertiga.

(3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadapa Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan,bank sentral, perbankan, keuangan, lembaga

internasioanal, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga.

(4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga."[16]

1.5.4. Sejarah Komputer

Internet merupakan hasil pemikiran yang visioner dari sejumlah pakar pada permulaan 1960-an. Mereka melihat adanya nilai potensial apabila komputer dapat digunakan untuk berbagai informasi mengenai hasil penelitain dan perkembangan (research & development) dibidang keilmuan dan militer. J.C.R Licklider dari MIT adalah yang pertama-tama menyarankan agar dibangun suatu jaringan global Internet (global network of computers) pada 1962. Licklider akhirnya pindah ke Defense Advanced Projects Agency (DAPRA) pada akhir 1962 untuk memimpin tugas mengembangkan pemikirannya itu.

Leonard Kleinrock dari MIT yang kemudian bekerja di UCA, mengembangkan suatu teori yang dikenal sebagai theory of packet switching. Teori ini dimaksudkan untuk membangun dasar bagi hubungan-hubungan Internet. Lawrence Roberts dari MIT berhasil menghubungkan komputer di Massachusetts dengan suatu komputer di California pada 1965 melalui jalur telepon dial-up. Hal yang dilakukan oleh Lawrence Roberts tersebut di suatu pihak menunjukkan dimungkinkannya dibangun

[16] Aziz Syamsuddin, Tindak Pidana Khusus, Sinar Grafika, Cet I, Jakarta, 2011, hlm. 123 -130

suatu Wide Area Networking tetapi di pihak lain juga menunjukkan bahwa telephone line's circuit switching dapat digunakan untuk membangun hubungan-hubungan komputer secara lebih luas. Dengan demikian, packet switching theory yang dikembangkan oleh Kleinrock memperoleh konfirmasi. Lawrence Roberts pada 1966 pindah ke DAPRA dan mengembangkan rencananya untuk kepentingan APRANET. Mereka itu dan banyak lagi yang tidak dapat disebut namanya satu persatu dalam tulisan ini merupakan para penemu sebenarnya dari Internet.

Internet yang kemudian dikenal sebagai APRANET berhasil online pada 1969 berdasarkan suatu kontrak yang dibuat oleh Advenced Research Projects Agency (APRA). Pada mulanya baru menghubungkan empat buah komputer utama pada beberapa universitas di bagian south western (barat daya) Amerika Serikat, yaitu UCLA, Stanford Research Institute, USCB, dan University of Utah. Kontrak tersebut dilaksanakan oleh BBN of Cabridge, MA di bawah Bob Kahn dan menjadi online pada Desember 1969. Pada Juni 1970, MIT, Harvard, BBN, dan Systems Development Corp. (SDC) di Santa Monica, California bergabung pula. Pada Januari 1971, Menyusul bergabung Standford, Lincoln Labs dari MIT, Carnegie-Mellon, dan Case-Western Reserve University. Pada bulan-bulan berikutnya NASA/Ames, Mitre, Burrough, RAND, dan University of Illinois bergabung. Setelah itu bergabung banyak lagi institusi yang tentu saja tidak mungkun ditulis nama-namanya.

Internet dirancang antara lain untuk menciptakan suatu jaringan komunikasi yang dapat bekerja sekalipun seandainya salah satu situs rusak akibat serangan nuklir. Apabila kebanyakan direct route tidak bekerja, maka routers akan mengarahkan lalu lintas pesan yang dikirimkan dan diterima itu melalui jalur-jalur alternatif. Internet di masa permulaannya digunakan oleh para pakar komputer, insinyur, ilmuwan, dan para pustakawan. Pada waktu itu, komputer belum semudah sekarang. Belum ada home computer atau personal computer sehingga setiap orang yang menggunakan komputer harus belajar suatu sistem yang sangat rumit.[17]

1.5.5. Internet Melahirkan Kejahatan Komputer

Di samping menciptakan berbagai peluang baru dalam kehidupan masyarakat, Internet juga sekaligus menciptakan peluang-peluang baru bagi kejahatan. Di dunia virtual orang melakukan berbagai perbuatan jahat (kejahatan) yang justru tidak dapat dilakukan di dunia nyata. Kejahatan tersebut dilakukan dengan menggunakan komputer sebagai sarana perbuatannya.

Antara 20 September dan 1 November 2004 The Pew Internet Project melakukan online survey yang diikuti oleh 1.286 ahli. Menurut hasil penelitian tersebut, dalam waktu 10 tahun mendatang Internet akan menjadi demikian pentingnya bagi para pengguna komputer sehingga

[17] Sutan Remy Syahdeini, Kejahatan dan Tindak Pidana Komputer, PT Pustaka Utama Grafiti, Cet I, Jakarta, 2009, hlm. 9-10

jaringan Internet akan menjadi sasaran yan sangat mengundang bagi serangan kejahatan komputer.

Kejahatan yang dilakukan di dunia virtual dengan menggunakan komputer itu disebut “kejahatan komputer” atau “cyber crime”. Istilah tersebut dilawankan dengan istilah “kejahatan tradisional” atau “real-world crime.”

Sebagian besar anak muda dan para remaja memiliki dan/atau dapat menggunakan komputer. Hal ini tidak terkecuali pula dengan Indonesia. Di Amerika Serikat terdapat 80 juta orang dewasa dan 10 juta anak-anak yang mampu mengakses Internet. Keadaan ini tentu saja telah memarakkan terjadinya kejahatan komputer.

Kejahatan-kejahatan komputer yang dimaksud diantaranya adalah cyber squatting, identify theft, kejahatan kartu kredit (carding), phishing, hacking, cyberterrorism, DOS dan DDOS attack, online gambling, penyebaran malware, pencurian data dan informasi elektronik, memodifikasi data dan informasi elektronik, penggandaan program komputer secara tidak sah, pornografi anak (child pornography), dan cyberstalking.

Kejahatan-kajahatan komputer telah menciptakan masalah-masalah beru bagi tugas penyelidikan, penyidikan, dan penuntutan oleh para

penegak hukum. Konsekuensinya, electronic information dan electronic transaction memerlukan adanya perlindungan yang kuat terhadap upaya-upaya yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab untuk dapat mengakses informasi yang tersimpan dalam sistem komputer. Kebutuhan perlindungan yang demikian ini menjadi sangat tinggi apabila menyangkut electronic information yang sifatnya sangat rahasia.[18]

1.5.6. Kejahatan Perbankan Dalam Problematika Perkembangan Hukum Ekonomi Dan Teknologi

a) Sistem Transfer Dana Elektronik dan Pengaruh Terhadap Kegiatan Perbankan/Perekonomian

Kehidupan dunia modern saat ini tidak dapat dihindari dan bahkan sering sangat bergantung , pada aktivitas dan jasa perbankan.Berbagai kegiatan / kepentingan (baik untuk kepentingan pribadi atau kepentingan umum diberbagai sektor kehidupan) sangat memerlukan jasa perbankan, khususnya yang terkait dengan dana uang tunai atau uang yang tersimpan dalam rekening pada suatu bank). Oleh karena itu kegiatan transfer dana (pemindahan / pengiriman / pembayaran / uang) merupakan salah satu kegiatan yang sangat penting dalam kehidupan modern saat ini.

Perkembangan globalisasi di berbagai bidang kehidupan yang ditunjang dengan pesatnya kemajuan teknologi informasi dan elektronik telah memunculkan sistem transfer dana elektronik (Elektronik Found Transfer

[18] Ibid, hlm. 8-9

System, disingkat EFTS).[19] Sehubungan dengan perkembangan teknologi canggih dan berkembangnya EFTS itu, muncul pulalah berbagai kegiatan perbankan dan perdagangan/perekonomian dengan teknologi canggih (high tech).misalnya Internet Banking, Cyber Bank, Elektronik and Cyber Space Comerce, Online Business, dan sebagainya.

(b) Kejahatan Transfer Dana Elektronik (EFT Crime) : Salah Satu Bentuk Kejahatan Teknologi Canggih (Hight Tech Crime)

Berkembangnya teknologi canggih dan sistem transfer dana elektronik (EFTS: Electronik Funds Transfer System) diikuti pula dengan berkembangnya kejahatan teknologi canggih (hight tech crime).Dikenal antara lain istilah cyber crime, EFT crime, cybank crime, internet banking crime, onLine business crime, cyber/electronik money laundring, hight tech WWW (white collar crime), bank fraud (penipuan bank, termasuk penipuan ATM; credit card fraud, insurance fraud, stock market fraud, investment related fraud, online fraud dan sebagainya.[20]

1.5.7. Pembedaan Hacker Dan Cracker

Sampai saat ini sering terdapat kekeliruan dalam menuliskan istilah yang tepat untuk mereka yang melakukan perusakan terhadap situs milik publik atau pribadi. Istilah yang sering digunakan oleh media cetak dan

[19] Barda Nawawi Arief, op. cit. hlm. 52
[20] Ibid, hlm. 54

elektronik adalah hacker, padahal yang tepat adalah cracker.[21] Kesalahan penggunaan istilah ini menyebabkan apa yang dipahami oleh masyarakat mengenai gambaran tingkah laku hacker adalah negatif. Untuk itulah pemahaman mengenai perbedaan antara hacker dan cracker diperlukan dalam pembahasan ini agar tidak terjadi atau tercipta pengertian yang salah mengenai makna hacker dan cracker.

Untuk memahami pembedaan dan penggunaan kedua istilah tersebut maka dipandang perlu untuk melihatnya dari sisi sejarah perkembangan dan penggunaan istilah tersebut. Sejarah hacker sendiri tidak bisa dilepaskan dari sejarah perkembangan komputer dan jaringan komputer. Secara umum sejarah hacker dapat dibagi dalam 3 (tiga) gelombang, yaitu:[22]

a. Hacker Gelombang Pertama

Hacker gelombang pertama atau awal perkembangan hacker terpusat di sekitar Massachusetts Institute of Technology (MIT) yang memiliki rasa ingin tahu dan kepandaian untuk mengeksplorasi peralihan jaringan telepon (the phone switching networks) dan sistem kontrol pada Tech Model Railroad Club dan menyusun komputer di Massachusetts Institute of Technology Artificial Intelegence Laboratorium (MIT Al Lab). Direktur laboratorium itu, Marvin Minsky, menaruh simpati dan cukup

[21] Agus Raharjo, Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi, PT Citra Aditya Bakti, Cet I, Bandung, 2002, Hal. 134

[22] Ibid, Hal. 135

berkesan dengan keinginan dan kepandaian para hacker untuk mengeksplorasi hal tersebut di atas. Dia juga mengijinkan para hacker itu secara langsung menghubungkan (access) dengan mesin. Di antara para hacker itu telah keluar dari sekolah (dropped out) dan menghabiskan waktunya untuk melakukan kegiatan hacking. Termasuk figure hacker legendaris pada gelombang pertama ini adalah Peter Deutsch, Bill Grosper, Richard Greenblatt, Tom Knight dan Jerry Sussman.Waktu itu adalah usia emas para hacker komputer, meskipun pada saat itu para hacker dihadapkan pada persoalan keadaan mesin, yaitu mesin yang besar, lambat, tidak praktis untuk dipergunakan dan kelihatannya memerlukan usaha yang keras untuk membuat komputer itu dapat bekerja secara sederhana untuk menghitung.Meskipun kejadian tersebut telah berlangsung lebih dari 40 (empat puluh) tahun yang lalu, para programer saat ini menyukai usaha mereka dan melihatnya melalui cerita mengenai asal mula penghitungan dengan mesin yang digunakan terlihat primitif dan lebih layak untuk dibuang.

b. Hacker Gelombang Kedua

Komputer dengan cepat menyebar ke negara bagian lain di Amerika Serikat, demikian juga dengan budaya hacker. Sebagian besar penyebarannya adalah inisiatif dari hacker yang telah mulai di Massachusetts Instituttte of Technology (MIT). Pada pertengahann1960-an terlihat pusat pengembangan budaya hacker ada di universitas lain,

seperti Carnegie Mellon University dan Stanford University. The Stanford Al Lab (SAIL) di bawah direksi John McCarthy, menjadi pusat aktivitas hacker di pesisir barat Amerika Serikat. Ketika mesin The Stanford Al Lab (SAIL) akhirnya mati (shut down) pada 1991, para hacker mengirim e-mail yang berisi pesan selamat tinggal kepada internet sebagaimana mesin The Stanford Al Lab (SAIL) itu mengirimkan ucapan terakhir kepada teman. Pada waktu itu setiap pusat penelitian (untuk kepentingan) komersial menjadi rumah bagi hacker. Perusahaan-perusahan seperti ATT, Xerox dan lainnya semuanya mempunyai programmer yang mempunyai keahlian untuk menjadi hacker. Termasuk dalam hacker legendaris gelombang kedua dan aktif beraktivitas antara lain Ed Fredkin, Brian Reid, Jim Gosling, Brian Kernighan, Dennis Ritchie dan Richard Stallman.

c. Hacker Gelombang Ketiga

Gelombang ketiga dari aktivitas hacker lahir di California sebelah utara tanpa ada hubungan langsung (silsilah) dengan hackers Massachusetts Institute of Technology (MIT). Hacker ini di mulai dengan Himebrew Computer Club di San Fransisco. Klub ini adalah kelompok pecinta elektronik dengan kebiasaan menarik dan mempu nyai ide radikal untuk membangun komputer mereka.Karena persoalan ukuran dan harga dari komputer terbaru, maka setiap hacker membatasi penggunaan angka kecil (small number) dari mesin yang dibangun oleh perusahaan besar dan

menginstal di univesitas atau pusat penelitian industri. Hacker gelombang ketiga ingin menginginkan mesin mereka tidak hanya dapat diprogram di rumah, tetapi dibangun dan dimodifikasi dengan hardware komputer dari rumah.Mereka yang termasuk kelompok hacker gelombang ketiga dan termasuk figur legendaris adalah Lee Felsenstein, Steve Dompier,Steve Wozniak, Steve Jobs dan Bill Gates.

Hacker gelombang pertama adalah sekelompok orang yang pertama kali menggunakan hack untuk teknik-teknik yang dipakai pada pemrograman kreatif yang mampu memecahkan masalah secara lebih efisien dari pada teknik biasa. Hacker –hacker ini lah yang membantu pengembangan bahasa LISP (bahasa pada sistem atau program komputer) yang diciptakan oleh John McCarthy, Direksi The Stanford Al Laboratorium.[23]

Hacker gelombang kedua telah berhasil membuat sistem operasi sendiri untuk mini komputer mereka dan membuat berbagai program. Perkembangan yang menarik pada gelombang ini adalah kelahiran sistem opersasi UNIX karya Ken Thompson dan Dennis Ritchie. Sistem operasi inilah yang kemudian dalam perkembangannya digunakan secara umum untuk membangun jaringan komputer, baik local maupun wide area network. Dennis Ritche juga menciptakan bahasa C (yang merupakan pengembangan bahasa pemrograman B yang diciptakan oleh Ken

[23] Ibid, Hal. 137

Thompson) yang digunakan untuk sistem operasi UNIX yang amat populer dan mempermudah para programer dan hacker[24]

Setelah komputer yang berukuran raksasa telah digantikan oleh komputer pribadi yang berukuran lebih kecil dan telah menyebar kerumah-rumah sebagai akibat penemuan komputer pribadi itu oleh Steve Jobs dan Steve Wozniack maka jumlah hacker semakin meningkat dengan sendirinya . Hacker pada masa ini (gelombang ketiga) berbeda dengan hacker pada sebelumnya (di Massachusetts Institute of Technology (MIT)) karena hacker masa ini lebih sering berkutat dengan perangkat lunak.Sebagian dari hacker gelombang ketiga ini kemudian sukses menjadi usahawan di bidang komputer, seperti Bill Gates dengan Microsoft-nya Steven Wozniak dan Steve Jobs melalui Apple Computer-nya[25]

Sebenarnya , sejarah perkembangan hacker tidak terbatas pada ketiga gelombang tersebut, karena pada tahun 1990-an muncul gelombang baru perkembangan hacker. Akan tetapi, pada tahun 1990-an ini istilah hacker semakin buruk karena dikonotasikan sebagai orang-orang jahat yang melakukan perusakan terhadap situs milik publik atau pribadi. Jumlah mereka atau cracker dari tahun ke tahun mengalami penambahan yang oleh hacker sejati tidak bisa dibendung. Mereka tergabung dalam

[24] Ibid.
[25] Ibid, Hal. 138

berbagai kelompok –kelompok hacker underground. Mereka yang masuk dalam gelombang ini (tanpa membedakan hacker dan cracker), antara lain Robert Tappan Morris, Kevin Minick, Tsutomu Shimomura dan masih banyak lagi.

Dalam sejarah hacker, apa yang dilakukan oleh para hacker itu selalu ada kaitannya dengan pengembangan sistem keamanan komputer. Keamanan komputer itu penting untuk melindungi data-data informasi yang bersifat rahasia dan agar tetap terjaga kerahasiaannya maka sistem keamanan yang ada dan digunakan untuk melindunginya perlu secara terus menerus dimodifikasi atau selalu dijaga kemutakhiran. Tugas hacker adalah menguji sistem keamanan dan memperbaikinya sistem atau programer (tetapi tidak semua programer bisa menjadi hacker).

Yang membedakan antara hacker dengan cracker yang utama adalah dalam hal niat. Hacker (atau disebut dengan hacker topi putih) mempunyai niat yang luhur, sedangkan cracker mempunyai niat jahat berupa keinginan untuk merusak atau menguasai atau ingin memiliki sesuatu. Perbedaan kedua adalah dalam masalah kemampuan, cracker tidak harus atau tidak selalu memiliki kemampuan seperti yang dimiliki oleh hacker seperti (pemrograman), tetapi seorang hacker sejati adalah seorang programer. Perbedaan ketiga dalam hal sifat Hacker selalu memegang teguh sifat atau prinsip-prinsip seorang hacker (seperti telah disebutkan diatas), tetapi cracker tidak memilki(atau memiliki tetapi tidak

mematuhi) sifat seperti hacker. Perbedaan keempat adalah dalam masalah etika. Hacker selalu memegang teguh dan mematuhi etika hacker dalam melakukan aktivitasnya, sedangkan cracker dalam melakukan aksinya sama sekali tidak mematuhi etika tesebut . Bagi cracker etika bukanlah prinsip atau pedoman tingkah laku yang harus dituruti atau diikuti , melainkan rasa senang dan kebanggan bisa membobol atau merusak situs milik orang atau badan hukum lain yang harus dijadikan pedoman aktivitasnya.

d. Hacking

Hacking adalah suatu perbuatan penyambun dengan cara menambah terminal komputer baru pada sistem jaringan komputer baru pada komputer tanpa izin (dengan melawan hukum) dari pemilik sah jaringan komputer.[26]

e. Cyber Squatting

Cyber squatting diartikan sebagai mendapatkan, memperjualbelikan, atau menggunakan suatu nama domain dengan itikad tidak baik atau jelek.[27]

---

[26] Andi Hamzah, Aspek-aspek Pidana di Bidang Komputer, Sinar Grafika, Jakarta, 1990. Hal. 38

[27] Abdul Wahid dan Mohammad Labib, Kejahatan Mayantara Cyber Crime , PT Refika Aditama, 2005, Hal. 63

f. Data Komputer Sebagai Bukti Dalam Perkara Pidana

Pasal 184 Kitab Undang – Undang Hukum Acara Pidana yang atau KUHAP menyebut tentang alat-alat bukti yang terdiri dari:

a. Keterangan.
b. Surat.
c. Keterangan ahli.
d. Petunjuk.
e. Keterangan terdakwa.[28]

1.5.8. Jenis-Jenis Cyber Crime Berdasarkan Modus Operandinya

1). Unauthorized Access to Computer System and Service (Tidak sah Akses ke Sistem Komputer dan Layanan)

Kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi Internet. Seperti halnya ketika masalah Timor Timur sedang hangat-hangatnya dibicarakan di tingkat internasional, beberapa website

[28] Andi Hamzah, Hukum Pidana Yang berkaitan Dengan Komputer, Sinar Grafika, Cet I Jakarta, 1993, Hal. 63

milik pemerintah RI dirusak oleh hacker (Kompas, 11/08/1999). Beberapa tahun lalu, hacker juga telah berhasil menembus masuk ke dalam data base berisi data para pengguna jasa America Online (AOL), sebuah perusahaan Amerika Serikat yang bergerak dibidang e-commerce yang memiliki tingkat kerahasiaan tinggi (Indonesian Observer, 26/06/2000). Situs Federal Bureau of Investigation (FBI) juga tidak luput dari serangan para hacker, yang mengakibatkan tidak berfungsinya situs ini beberapa waktu lamanya situsnya yaitu fbi.org.

2) Illegal Contents (Data Yang Tidak Benar)

Merupakan kejahatan dengan memasukkan data atau informasi ke Internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya, pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah dan sebagainya.

3) Data Forgery (Data Palsu)

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scripless document melalui Internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen e-commerce dengan membuat seolah-olah terjadi salah ketik yang pada

akhirnya akan menguntungkan pelaku karena korban akan memasukkan data pribadi dan nomor kartu kredit yang dapat saja disalah gunakan.

4) Cyber Espionage (Kejahatan Yang Melakukan Mata-Mata Dengan Pihak Lain)

Merupakan kejahatan yang memanfaatkan jaringan Internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network system) pihak sasaran.

Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data pentingnya (data base) tersimpan dalam suatu sistem yang computerized (tersambung dalam jaringan komputer)

5) Cyber Sabotage and Extortion (Kejahatan Yang Menyusupkan Data dan Pemerasan)

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan Internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu logic bomb, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku.

6) Offense against Intellectual Property (Pelanggaran Terhadap Kekayaan Intelektual)

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di Internet. Sebagai contoh, peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di Internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

7) Infringements of Privacy (Pelanggaran Privasi)

Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

1.5.9. Jenis-Jenis Cyber Crime Berdasarkan Motifnya

1) Cyber crime sebagai tindak kejahatan murni

Cyber crime jenis ini kejahatan yang dilakukan secara di sengaja, dimana orang tersebut secara sengaja dan terencana untuk melakukan pengrusakkan, pencurian, tindakan anarkis, terhadap suatu sistem informasi atau sistem komputer.

2) Cyber crime sebagai tindakan kejahatan abu-abu

Kejahatan ini tidak jelas antara kejahatan kriminal atau bukan karena dia melakukan pembobolan tetapi tidak merusak, mencuri atau

melakukan perbuatan anarkis terhadap system informasi atau system komputer tersebut.

1.5.10. Jenis-Jenis Cyber Crime Berdasarkan Korbanya

1) Cyber Crime Yang Menyerang Individu

Kejahatan yang dilakukan terhadap orang lain dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik, mencoba ataupun mempermainkan seseorang untuk mendapatkan kepuasan pribadi sebagai contoh misalnya menyebarkan foto-foto yang berbau pornografi melalui internet,membuat facebook dengan nama samaran yang digunakan untuk meneror ataupun kejahatan sejenisnya kepada seseorang dan lain sebagainya.

2) Cyber Crime Yang Menyerang Hak Cipta (Hak Milik)

Kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi atau umum ataupun demi materi maupun nonmateri.

3) Cyber Crime Yang Menyerang Pemerintah.

Kejahatan yang dilakukan dengan pemerintah sebagai objek dengan motif melakukan terror, membajak ataupun merusak keamanan suatu pemerintahan yang bertujuan untuk mengacaukan sistem pemerintahan, atau menghancurkan suatu negara.[29]

[29] Website : http://balianzahab.wordpress.com/ | Diskusi dan Konsultasi Masalah Hukum Di akses Pada Tanggal 15 Januari 2012 , Pukul 17:49 WIB

1.5.11. Kejahatan

Kejahatan merupakan Suatu fenomena yang komplek yang dapat dipahami dari berbagai sisi yang berbeda. Itu sebabnya dalam keseharian kita dapat menangkap berbagai komentar tentang suatu peristiwa kejahatan yang berbeda satu dengan yang lain. Kriminologi merupakan ilmu pngetahuan yang mempelajari tentang kejahatan. Nama kriminologi yang ditemukan oleh P. Topinard (1830-1911) seorang ahli antropologi Perancis, secara harfiah berasal dari kata" crimen" yang berarti kejahatan atau penjahat dan "logos" yang berarti ilmu pengetahuan, maka kriminologi dapat berarti ilmu tentang kejahatan atau penjahat.[30]

Secara formal kejahatan dirumuskan sebagai suatu perbuatan yang oleh Negara diberi pidana. Pemberian pidana dimaksudkan untuk mengembalikan keseimbangan yang terganggu akibat perbuatan itu. Keseimbangan yang terganggu itu ialah ketertiban masyarakat terganggu, masyarakat resah akibatnya. Kejahatan dapat didefinisikan berdasarkan adanya unsur anti sosial. Berdasarkan unsur itu dapatlah dirumuskan bahwa kejahatan adalah suatu tindakan anti sosial yang merugikan, tidak pantas, tidak dapat dibiarkan, yang dapat menimbulkan kegoncangan dalam masyarakat. Terdapat beberapa pendapat ahli mengenai kejahatan, di antaranya:

[30] Topo Santoso dan Eva Achjani Zulfa, Kriminologi, PT Raja Grafindo Persada, Jakarta, 2007, Hal. 9

a. D. Taft

”Kejahatan adalah pelanggaran hukum pidana”

b. Van Bemmelen

“Kejahatan adalah tiap kelakuan yang bersifat tidak susila dan merugikan, yang menimbulkan begitu banya ketidaktenangan dalam suatu masyarakat tertentu, sehingga masyarakat itu berhak untuk mencelanya dan menyatakan penolakannya atas kelakuan itu dalam bentuk nestapa dengan sengaja diberikan karena kelakuan tersebut”

c. Ruth Coven

“Orang berbuat jahat karena gagal menyeusaikan diri terhadap tuntutan masyarakat”

d. W.A. Bonger

“Kejahatan adalah perbuatan yang anti social yang oleh Negara ditentang dengan sadar dengan penjatuhan hukuman”[31]

1.5.12. Hubungan KUHP Dengan Cyber Crime

Kitab Undang-undang Hukum Pidana (KUHP) telah mengatur hubungan-hubungan hukum tentang kejahatan yang berkaitan dengan komputer (computer crime) yang kemudian berkembang menjadi cyber crime. Delik tentang pencurian dalam dunia maya termasuk salah satu delik yang paling populer diberitakan media masa. Pencurian disini tidak diartikan secara konvensional yakni tentang perbuatan mengambil barang secara nyata. Dalam kasus pencurian di Internet, barng yang dicuri yakni berupa data digital baik yang berisikan data transaksi keuangan milik orang lain.Delik pencurian diatur dalam Pasal 362 KUHP dan

[31] Ibid, Hal. 14

variasinya diatur dalam Pasal 363 KUHP,yakni tentang pencurian dengan pemberatan; Pasal 364 KUHP tentang pencurian ringan, Pasal 365, tentang pencurian yang disertai dengan kekerasan; Pasal 367 KUHP, tentang pencurian dilingkungan keluarga.Adapun bunyi dari pada pasal 362 adalah sebagai berikut;

"Barang siapa mengambil barang, yang sama sekali atau sebagian termasuk kepunyaan orang lain, dengan maksud akan memiliki barang itu dengan melawan hak, dihukum, karena pencurian, dengan hukuman penjara selama-lamanya lima tahun atau denda sebanyak-banyak sembilan ratus rupiah"

Menurut hukum pidana, pengertian benda diambil dari penjelasan Pasal 362 KUHP yaitu segala sesuatu yang berwujud atau tidak berwujud, (misalnya listrik) dan mempunyai nilai di dalam kehidupan ekonomi dari seseorang. Data atau program yang tersimpan di dalam media penyimpanan disket atau sejenisnya yang tidak dapat diketahui wujudnya dapat berwujud dengan cara menampilkan pada layar penampil komputer (screen) atau dengan cara mencetak pada alat pencetak (printer). Dengan demikian data atau program komputer yang tersimpan dapat dikategorikan sebagai benda seperti pada penjelasan Pasal 362 KUHP. Namun dalam sistem pembuktian kita terutama yang menyangkut elemen penting dari alat bukti (Pasal 184 KUHAP ayat (1) huruf c) masih belum mengakui data komputer sebagai bagiannya karena sifatnya yang digital. Padahal dalam kasus cyber crime data elektronik sering kali menjadi barang bukti yang ada.[32]

[32] http://forum.anugrahpratama.com/dunia-komputer/menjerat-pelaku-cyber-crime-dengan-kuhp/?wap2 Diakses Pada Tanggal 31 Januari 2012 Pukul 14.00 WIB

1.5.13. Tindak Pidana Perbankan

Adapun tindak pidana dibidang perbankan terdiri atas perbuatan-perbuatan yang melanggar hukum dalam ruang lingkup seluruh kegiatan usaha pokok lembaga keuangan bank sehingga perbuatan tersebut biasanya diancam dengan ketentuan pidana yang termuat diluar Undang-Undang No. 10 Tahun 1998 tentang perubahan atas Undang-Undang No. 7 Tahun 1992 tentang Pebankan, Undang-Undang perubahannya serta peraturan pelaksanaannya sehingga penindakannya berdasarkan delik biasa dan atau delik khusus.

Adapun ruang lingkup terjadinya tindak pidana perbankan, dapat terjadi pada keseluruhan lingkup kehidupan dunia perbankan dan lebih luasnya mencakup juga lembaga keuangan lainnya. Sedangkan ketentuan yang dapat dilanggarnya baik tertulis maupun yang tidak tertulis juga meliputi norma-norma kebiasaan pada bidang perbankan, namun semau itu tetap harus telah diatur sanksi pidananya. Lingkup pelaku dari tindak pidana perbankan dapat dilakukan oleh perorangan maupun badan hukum (korporasi).[33]

1.6. Metodologi Penelitian

a. Jenis dan Tipe Penelitian

Penelitian ini merupakan penelitian hukum normatif empiris (holistik/gabungan) yaitu pengkajian terhadap bahan – bahan hukum, baik

[33] Ronnny Prasetyo,Pembobolan ATM , Tinjauan Hukum Perlindungan Nasabah Korban Kejahatan Perbankan , Prestasi Pustaka, Cet I, Jakarta, 2004, Hal. 107

bahan hukum primer maupun bahan hukum sekunder dan mengkaji akibat/dampak hukumnya.[34]

Tipe penelitian studi kasus, "suatu gambaran hasil penelitian yang mendalam, dan lengkap, sehingga dalam informasi yang disampaikannya tampak hidup sebagaimana adanya dan pelaku – pelaku mendapat tempat untuk memainkan perannya".[35]

b. Sumber Data Hukum

Sumber data dalam penelitian ini yaitu menggunakan data sekunder adalah data dari penelitian kepustakaan dimana dalam data sekunder terdiri dari 3 (tiga) bahan hukum, yaitu bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier sebagai berikut :

1. Bahan Hukum Primer adalah bahan hukum yang sifatnya mengikat berupa peaturan perundang – undangan yang berlaku dan ada kaitannya dengan permasalahan yang dibahas. Terdiri dari

a) KUHP dan KUHAP (R. SOESILO)

[34] Bahder Johan Nasution, Metode Penelitian Ilmu Hukum, CV. Mandar Maju, Bandung, 2008, Hal. 97

[35] Burhan Ashshofa, Metode Penelitian Hukum, PT Rineka Cipta, Cet IV, Jakarta, 2010, Hal. 21

b) Undang – Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektonik (Departemen Komunikasi dan Informatika Republik Indonesia)

c) Undang – undang No. 10 Tahun 1998 Tentang Perbankan

2. Bahan Hukum Sekunder adalah bahan hukum yang sifatnya menjelaskan badan hukum primer, dimana bahan hukum sekunder berupa buku literatur, website, hasil karya sarjana. Terdiri dari :

a) Buku - buku tentang Hukum Pidana;

b) Buku - buku tentang Cyber Crime;

c) Buku - buku tentang Penelitian Hukum;

d) Buku - buku tentang Penelitian Hukum Normatif

e) Buku - Metodologi Penelitian Hukum;

f) Dokumen – dokumen di Kepolisian.

3. Bahan Hukum Tersier adalah bahan hukum sebagai pelengkap dari kedua bahan hukum sebelumnya, yaitu kamus hukum dan hasil wawancara atau pengamatan secara empiris sebagai penunjang untuk memberikan gambaran secara komprehensif baik secara normatif maupun sosiologis atau empiris.

c. Metode Pengumpulan Data Hukum

Metode yang digunakan dalam pengumpulan data ini diambil dari bahan – bahan hukum sebagai kajian normatif sebagian besar diperoleh

melalui dokumen hukum, antara lain Peraturan perundang – undangan, buku – buku ilmu hukum, dan jurnal hukum.[36]

d. Metode Pengolahan Data Hukum

Analisis data merupakan proses yang tidak pernah selesai. Proses analisis data itu sebenarnya merupakan pekerjaan untuk menemukan tema – tema dan merumuskan hipotesa – hipotesa, meskipun sebenarnya tidak ada formula yang pasti untuk dapat digunakan untuk merumuskan hipotesa. Hanya saja pada analisis data tema dan hipotesa lebih diperkaya dan diperdalam dengan cara menggabungkannya dengan sumber – sumber data yang ada.[37]

e. Metode Analisis Data Hukum

Penelitian ini peneliti menggunakan metode kualitatif. Pengertian metode kualitatif menurut Soerjono Soekanto adalah "suatu tata cara penelitian yang menghasilkan data deskriptif analitis, yaitu apa yang dinyatakan responden secara tertulis maupun lisan, dan perilaku nyata...".[38]

[36] Bahdar Johan Nasution, Metode Penelitian Ilmu Hukum, CV. Mandar Maju, Bandung, 2008, Hal.98

[37] Burhan Ashshofa, op.cit.Hal 66

[38] Soerjono Soekanto, Pengantar Penelitian Hukum, Universitas Indonesia, Jakarta, 1984, Cet III, Hal. 250

f. Sistematika Penulisan

Pemaparan dari sistematika penulisan ini bertujuan supaya di dalam proses penyampaian materi dari skripsi ini dapat mudah dipahami. Sistematika penulisan skripsi ini dibagi menjadi empat bab, pada tiap bab terdiri dari beberapa sub bab, yaitu :

Bab I menjelaskan tentang pendahuluan, yang meliputi : latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, kajian pustaka, metodologi penelitian dan sistematika penulisan.

Bab II menjelaskan tentang akibat hukum dari pembobolan mesin ATM Bank menurut hukum pidana, yang meliputi : pengertian hukum dan akibat hukum dari pembobolan ATM Bank menurut hukum pidana.

Bab III menjelaskan tentang perlindungan hukum bagi nasabah yang menjadi korban pembobolan mesin ATM Bank, yang meliputi : perlindungan hukum yang diberikan pihak bank kepada pengguna ATM yang menjadi nasabah dan perlindungan hukum bagi nasabah yang menjadi korban pembobolan mesin ATM bank.

Bab IV menjelaskan tentang penutup, yang meliputi kesimpulan dan saran.